Nathan R. Ring,
Nevada State Bar No. 12078
STRANCH, JENNINGS & GARVEY, PLLC
3100 W. Charleston Boulevard, Suite 208
Las Vegas, NV 89102
Telephone: (725) 235-9750
lasvegas@stranchlaw.com

Sabita J. Soneji (*pro hac vice forthcoming*)
TYCKO & ZAVAREEI LLP
1970 Broadway, Suite 1070
Oakland, CA 94612
Phone: (510) 254-6808
ssoneji@tzlegal.com

F. Peter Silva, II (*pro hac vice forthcoming*)
TYCKO & ZAVAREEI LLP
2000 Pennsylvania Avenue, NW, Suite 1010
Washington, D.C. 20006
Phone: (202) 973-0900
psilva@tzlegal.com

Counsel for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA

DHAMAN GILL, *individually and on behalf of all others similarly situated*, Plaintiff, v. **CAESARS ENTERTAINMENT, INC.**, Defendant.	**Case No.** **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Dhaman Gill ("Plaintiff" or "Mr. Gill"), individually on and on behalf of all similarly situated persons, by and through his undersigned counsel, files this Class Action Complaint against Caesars Entertainment, Inc. ("Caesars" or "Defendant") and alleges the following based on personal

knowledge of facts pertaining to her, on information and belief, and based on the investigation of counsel as to all other matters.

NATURE OF THE ACTION

1. Caesars is a gaming and hospitality company that owns, leases, brands, or manages 53 domestic properties in 18 states including Caesars Palace located on the Las Vegas Strip as well as operating online gambling sites throughout the country. Caesars is a publicly traded company and listed on the NASDAQ stock exchange with the ticket symbol "CZR". [1]

2. This class action arises out of a recent cyberattack and data breach ("Data Breach"), which resulted in unauthorized actors viewing and accessing the personally identifiable information ("PII") of significant number of individuals who were members of Caesars's loyalty program.[2]

3. On or before September 7, 2023, Caesars identified suspicious activity in its IT network resulting from a social engineering attack on an outsourced IT support vendor used by the company. Through its investigation, Caesars determined that an unauthorized actor acquired, among other data, a copy of its loyalty program database including driver's license numbers and Social Security numbers of its members. [3] According to its online notice, Caesars is still investigating whether any other additional data, or otherwise sensitive data was taken.[4]

4. Caesars's carelessness, negligence, and lack of oversight and supervision caused its

---

[1] Form 10-Q, U.S. SEC. AND EXCH. COMM'N (Aug. 1, 2023), https://www.sec.gov/ix?doc=/Archives/edgar/data/1590895/000159089523000091/czr-20230630.htm (last visited Oct. 3, 2023).
[2] *See* Caesars's Online Notice, Learn More, https://response.idx.us/caesars/#learn-more (last visited Oct. 3, 2023).
[3] SEC Form 8-K, Caesars Entertainment, Inc. (Sept. 7, 2023), https://www.sec.gov/Archives/edgar/data/1590895/000119312523235015/d537840d8k.htm (last visited Oct. 4, 2023).
[4] Caesars's Online Notice, *supra* n. 2.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

customers to lose all sense of privacy. Plaintiff and members of the Class have suffered irreparable harm, including the exposure of their PII to nefarious strangers and their significantly increased risk of identity theft. The information at issue here is the very kind of information that allows identity thieves to construct false identities and invade all aspects of Plaintiff's and Class members' lives. In addition to facing the emotional devastation of having such personal information fall into the wrong hands, Plaintiff and Class members must now undertake additional security measures and precautions to minimize their risk of identity theft.

5. Plaintiff's and the Class members' rights were disregarded by Caesars's negligent or reckless failure to take adequate and reasonable measures to ensure its data systems were secure and the PII entrusted to it would not be stolen. Caesars also failed to disclose the material fact that it did not have adequate information security controls to safeguard PII, failed to supervise its third-party vendors, failed to take foreseeable steps to prevent the Data Breach, and failed to monitor and timely detect the Data Breach.

6. As a result of the Data Breach, Plaintiff's and Class members' PII has been and will continue to be exposed to criminals for misuse.

7. Plaintiff brings this action individually and on behalf of the Class, seeking remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, injunctive relief, reasonable attorneys' fees and costs, and all other remedies this Court deems proper.

PARTIES

Plaintiff

8. Plaintiff Dhaman Gill is a citizen and resident of the state of California. Plaintiff is a member of Caesars's loyalty program, Caesars Rewards.

9. On September 14, 2023, Caesars filed a Form 8-K with the United States Security

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

and Exchange Commission ("SEC") to report that the Data Breach, a material event, had occurred. Caesars reported an "unauthorized actor acquired a copy of, among other data, [its] loyalty program database, which includes driver's license numbers and/or Social Security numbers for a significant number of members in the database."[5]

10. Plaintiff has been a Caesars loyalty member for at least six years and entrusted Caesars with his personal information, including his name, address, driver's license number, email address, phone number, Social Security number, and date of birth.

11. In its privacy policy, Caesars represented to Plaintiff and Class members that it is committed to respecting Plaintiff and Class members' data privacy, and that it maintained "physical, electronic and organizational safeguards that reasonably and appropriately protect against the loss, misuse and alteration of the information under our control."[6]

12. Plaintiff and Class members entrusted confidential PII to Caesars for purpose of participating in its loyalty program with the reasonable expectation, and mutual understanding, that Caesars would comply with its obligations to keep such information confidential and secure from unauthorized access, including thoroughly vetting all third parties it hired to ensured that they employed adequate data security measures, procedures, protocols, and practices.

13. Because of the Data Breach, Plaintiff's PII is now in the hands of criminals. Plaintiff and all Class members are now imminently at risk of crippling future identity theft and fraud.

14. After learning of the Data Breach, Plaintiff spent considerable time investigating the Data Breach. For instance, Plaintiff has spent time research the legitimacy of the Data Breach and taking other steps in an attempt to mitigate the adverse consequences of the Data Breach including changing passwords to his online accounts and placing a credit freeze on his credit. The

[5] SEC Form 8-K, *supra* n. 3.
[6] https://www.caesars.com/corporate/privacy (last visited Oct. 10, 2023).

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

Online Notice directed Plaintiff to take these actions.[7]

15. As a direct and proximate result of the Data Breach, Plaintiff will likely need to purchase a lifetime subscription for identity theft protection and credit monitoring.

16. Plaintiff has been careful to protect and monitor his identity. Plaintiff has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable PII; (b) damages to and diminution in value of Plaintiff's PII that was entrusted to Caesars with the understanding that Caesars would safeguard this information against disclosure; (c) loss of the benefit of the bargain with Caesars to provide adequate and reasonable data security—i.e., the difference in value between what Plaintiff should have received from Caesars and Caesars's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security and failing to protect Plaintiff's PII; and (d) continued risk to Plaintiff's PII, which remains in the possession of Caesars and which is subject to further breaches, so long as Caesars fails to undertake appropriate and adequate measures to protect the PII that was entrusted to Caesars.

Defendant

17. Defendant Caesars Entertainment Inc. is a Delaware corporation with its principal place of business located at 100 West Liberty Street, 12th Floor, Reno, Nevada 89501. Caesars can be served via its registered agent, Corporation Service Company, 112 North Curry Street, Carson City, Nevada 89703.

JURISDICTION AND VENUE

18. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs.

[7] *See* Caesars's Online Notice, *supra* n. 2.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

At least one member of the Class, defined below, is a citizen of a different state than Defendant, and there are more than 100 putative Class members.

19. This Court has personal jurisdiction over Defendant because its principal place of business is in this District, it regularly transacts business in this District, and upon information and belief, some Class members reside in this District.

20. Venue is proper in this District under 28 U.S.C. § 1391(a)(1) because Defendant's principal place of business is located in this District and a substantial part of the events giving rise to this action occurred in this District.

FACTUAL ALLEGATIONS

The Data Breach

21. On or before September 7, 2023, Caesars identified suspicious activity in its IT network resulting from a social engineering attack on an outsourced IT support vendor used by the Company. Through its investigation, Caesars determined that an unauthorized actor acquired, among other data, a copy of its loyalty program database including driver's license numbers and Social Security numbers. The Data Breach may have included the PII of tens of millions of Caesars loyalty members.[8]

22. According to news reports, the unauthorized actor is a hacking group known as Scattered Sider (or UNC3944) which is known for using social engineering to trick employees of the target company into granting them access to their network.[9] It has also been reported that Caesars paid as much as $15,000,000.00 to the unauthorized actor as ransom following the Data

[8] https://fortune.com/2023/09/15/caesars-entertainment-cyberattack-mgm-resorts-data-breach/ (last visited Oct. 10, 2023).

[9] https://techcrunch.com/2023/09/14/caesars-entertainment-data-breach-cyberattack/ (last visited Oct. 10, 2023).

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

Breach.[10]

23. On or around September 14, 2023, Caesars filed a Form 8-K with the SEC to alert investors and shareholders that the Data Breach represented a material event that could materially affect the value of the company.[11]

24. Also, around that time, Caesars published an informational website regarding the Data Breach. While the website did not provide much detail about the scope and breadth of the Breach, it did state that at a minimum the driver's license numbers and Social Security numbers of loyalty program members had been accessed.[12] Caesars stated that it is offering credit monitoring and identity theft protection services to all loyalty program members. However, Caesars has failed to adequately inform victims that their private information had been breached and instead placed the burden on loyalty members to investigate what happened and possibly stumble onto its informational website. Caesars has yet to send notices to Plaintiff or Class member to personally and specifically inform them that their PII – and what other PII -- was compromised in the Data Breach.

25. Caesars is responsible for allowing the Data Breach to occur because it failed to implement and maintain reasonable safeguards, failed to comply with industry-standard data security practices, as well as federal and state laws and regulations governing data security, and failed to supervise, monitor, and oversee all third parties it hired who had access to Plaintiff's and the Class members' PII.

26. During the Data Breach, Caesars failed to adequately monitor its information technology infrastructure and its third-party IT support vendor. Had Caesars done so, it would have

---

[10] https://nypost.com/2023/09/14/caesars-entertainment-paid-about-15m-to-hackers-who-stole-customer-social-security-numbers-other-info-report/ (last visited Oct. 10, 2023).

[11] SEC Form 8-K, *supra* n. 3.

[12] *See* Caesars's Online Notice, *supra* n. 2.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

prevented or mitigated the scope and impact of the Data Breach.

27. Plaintiff and Class members provided their PII to Caesars with the reasonable expectation and mutual understanding that Caesars would comply with its obligations to keep such information confidential and secure from unauthorized access.

28. Caesars's data security obligations were particularly important given the substantial increase in cyber and ransomware attacks and data breaches in the gaming and hospitality industries preceding the date of the Data Breach, as well as given the incredibly sensitive nature of PII that it retained in its servers.

29. By obtaining, collecting, and using Plaintiff's and Class members' PII, Caesars assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class members' PII from disclosure.

30. As a result of Caesars's failure to protect sensitive PII it was entrusted with, Plaintiff and Class members are at a significant risk of identity theft, financial fraud, and other identity-related fraud into the indefinite future. Plaintiff and Class members have also lost the inherent value of their PII.

Caesars Was on Notice of Data Breach Threats and the Inadequacy of Its Data Security

31. Caesars's data security obligations were especially important given the substantial increase in cyberattacks and data breaches in recent years. In 2022, there were 1,802 reported data breaches, affecting approximately 422 million individuals.[13]

32. Caesars should have been aware—and was aware—that it was at risk of an internal data breach that could expose the PII that it collected and maintained.

[13] *2022 Data Breach Report*, IDENTITY THEFT RES. CTR., https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf, at 2 (last visited Aug. 15, 2023).

SJG STRANCH, JENNINGS & GARVEY PLLC
3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com

33. Despite this, Caesars failed to take the necessary precautions required to safeguard Plaintiff's and Class members' PII from unauthorized access.

Caesars Failed to Comply with Statutory and Regulatory Obligations

34. Federal and State governments have established security standards and issued recommendations to minimize data breaches and the resulting harm to individuals and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for businesses that highlight the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[14]

35. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which establishes guidelines for fundamental data security principles and practices for business.[15] Among other things, the guidelines note businesses should properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating that someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[16]

36. Additionally, the FTC recommends that companies limit access to sensitive data, require complex passwords for network access, use industry-tested methods for security, monitor

---

[14] *See Start With Security: A Guide for Business*, FTC (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205- startwithsecurity.pdf (last visited Oct. 10, 2023).

[15] *Protecting Personal Information: A Guide for Business*, FTC (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited Oct. 10, 2023).

[16] *Id.*

3100 W. Charleston Blvd., #208 Las Vegas, NV 89102 SJG STRANCH, JENNINGS & GARVEY PLLC 725-235-9750 lasvegas@stranchlaw.com

for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.[17]

37. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect PII, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[18]

38. Caesars also failed to comply with commonly accepted industry standards for data security. Security standards commonly accepted among businesses that store PII using the internet include, without limitation:

- Maintaining a secure firewall configuration;
- Maintaining appropriate design, systems, and controls to limit user access to certain information as necessary;
- Monitoring for suspicious or irregular traffic to servers;
- Monitoring for suspicious credentials used to access servers;
- Monitoring for suspicious or irregular activity by known users;
- Monitoring for suspicious or unknown users;
- Monitoring for suspicious or irregular server requests;
- Monitoring for server requests for PII;
- Monitoring for server requests from VPNs; and

[17] *See Start With Security: A for Business*, FTC, *supra* n.14.

[18] *Privacy and Security Enforcement Press Releases*, FTC, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited Oct. 10, 2023).

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

- Monitoring for server requests from Tor exit nodes.

39. Caesars is also required by various states' laws and regulations to protect Plaintiff's and Class members' PII and to handle any breach of the same in accordance with applicable breach notification statutes.

40. In addition to its obligations under federal and state laws, Caesars owed a duty to Plaintiff and Class members whose PII were entrusted to Caesars to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Caesars owed a duty to Plaintiff and Class members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its systems and networks adequately protected the PII of Plaintiff and Class members.

41. Caesars owed a duty to Plaintiff and Class members whose PII was entrusted to Caesars to design, maintain, and test its systems to ensure that the PII in Caesars's possession was adequately secured and protected.

42. Caesars owed a duty to Plaintiff and Class members whose PII was entrusted to Caesars to create and implement reasonable data security practices and procedures to protect the PII in its possession.

43. Caesars owed a duty to Plaintiff and Class members whose PII was entrusted to Caesars to implement processes that would detect a breach on its data security systems in a timely manner.

44. Caesars owed a duty to Plaintiff and Class members whose PII was entrusted to Caesars to act upon data security warnings and alerts in a timely fashion.

45. Caesars owed a duty to Plaintiff and class members whose PII was entrusted to Caesars to disclose if its systems and data security practices were inadequate to safeguard

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

individuals' PII from theft because such an inadequacy would be a material fact in the decision to entrust PII to Caesars.

46. Caesars owed a duty to Plaintiff and Class members whose PII was entrusted to Caesars to disclose in a timely and accurate manner when data breaches occurred.

47. Caesars owed a duty of care to Plaintiff and Class members because they were foreseeable and probable victims of any inadequacy in its affirmative development of the systems to maintain PII and in its affirmative maintenance of those systems.

48. In this case, Caesars was fully aware of its obligation to use reasonable measures to protect the PII of its customers. Caesars also knew it was a target for hackers. But despite understanding the consequences of inadequate data security, Caesars failed to comply with industry-standard data security requirements.

The Effect of the Data Breach on Impacted Consumers

49. The exponential cost to Plaintiff and Class members resulting from the Data Breach cannot be overstated. Criminals can use victims' PII to open new financial accounts, incur charges in credit, obtain governmental benefits and identifications, fabricate identities, and file fraudulent tax returns well before a person whose PII was stolen becomes aware of it.[19] Any one of these instances of identity theft can have devastating consequences for the victim, causing years of often

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

[19] *See Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO-07-737 (June 2007), https://www.gao.gov/new.items/d07737.pdf (last visited Oct. 10, 2023); Melanie Lockert, *How do hackers use your information for identity theft?*, CREDITKARMA (Oct. 1, 2021), https://www.creditkarma.com/id-theft/i/how-hackers-use-your-information (last visited Oct. 10, 2023); Ravi Sen, *Here's how much your personal information is worth to cybercriminals – and what they do with it*, PBS (May 14, 2021), https://www.pbs.org/newshour/science/heres-how-much-your-personal-information-is-worth-to-cybercriminals-and-what-they-do-with-it (last visited Oct. 10, 2023); Alison Grace Johansen, *4 Lasting Effects of Identity Theft*, LIFELOCK BY NORTON (Feb. 4, 2021), https://lifelock.norton.com/learn/identity-theft-resources/lasting-effects-ofidentity-theft (last visited Oct. 10, 2023).

irreversible damage to their credit scores, financial stability, and personal security.

50. Defendant was or should have been aware that it was collecting highly valuable data, which has increasingly been the target of data breaches in recent years.

51. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

52. The exposure of any PII can cause unexpected harms one would not ordinarily associate with the type of information stolen. Cybercriminals routinely aggregate Private Information from multiple illicit sources and use stolen information to gather even more information through social engineering, credential stuffing, and other methods. The resulting complete dossiers of PII are particularly prized among cybercriminals because they expose the target to every manner of identity theft and fraud.

53. Identity thieves can use PII such as that exposed in the Data Breach to: (a) apply for credit cards or loans (b) purchase prescription drugs or other medical services (c) commit immigration fraud; (d) obtain a fraudulent driver's license or ID card in the victim's name; (e) obtain fraudulent government benefits or insurance benefits; (f) file a fraudulent tax return using the victim's information; (g) commit espionage; or (h) commit any number of other frauds, such as obtaining a job, procuring housing, or giving false information to police during an arrest.

Diminution of Value of PII

54. PII is valuable property.[20] Its value is axiomatic, considering the value of Big Data

[20] *See Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO-07-737 (June 2007), https://www.gao.gov/new.items/d07737.pdf, at 2 (last visited Oct. 10, 2023).

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

in corporate America and that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk-to-reward analysis illustrates, beyond doubt, that PII has considerable market value.

55. The PII stolen in the Data Breach is significantly more valuable than the loss of credit card information in a large retailer data breach. Victims affected by those retailer breaches could avoid much of the potential future harm by simply cancelling credit or debit cards and obtaining replacements.

56. This type of data commands a much higher price on the dark web. As Martin Walter, senior director at cybersecurity firm RedSeal, explained: "Compared to credit card information, personally identifiable information … [is] worth more than 10x on the black market."[21]

57. Sensitive PII can sell for as much as $363 per record according to the Infosec Institute.[22]

58. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly $200 billion.[23] Indeed, a Social Security number, date of birth, and full name can sell for $60 to $80 on the digital black market.[24]

---

[21] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT WORLD (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Oct. 10, 2023).

[22] *See, e.g.,* John T. Soma, et al., *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("Private Information") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3-4 (2009) ("Private Information, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[23] David Lazarus, *Column: Shadowy data brokers make the most of their invisibility cloak*, L.A. TIMES (Nov. 5, 2019), https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last visited Oct. 10, 2023).

[24] Michael Kan, *Here's How Much Your Identity Goes for on the Dark Web*, PCMAG (Nov. 15, 2017), https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web (last visited Oct. 10, 2023).

SJG STRANCH, JENNINGS & GARVEY PLLC
3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com

59. As a result of the Data Breach, Plaintiff's and Class members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

60. The fraudulent activity resulting from the Data Breach may not come to light for years.

61. Plaintiff and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiff and Class members are incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

62. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to millions of individuals' detailed PII and thus the significant number of individuals who would be harmed by the exposure of the unencrypted data.

63. The injuries to Plaintiff and Class members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class members.

Loss of Time to Mitigate the Risk of Identity Theft and Fraud

64. As a result of the recognized risk of identity theft, when a data breach occurs and an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

to greater financial harm.

65. Class members have spent, and will spend, time on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach upon seeing news reports, and monitoring their credit reports and financial accounts for suspicious activity, as Caesars advised in its online notice.[25]

66. These mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches, in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[26]

67. Plaintiff's mitigation efforts are also consistent with the steps the FTC recommends data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (and considering an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[27]

68. Plaintiff and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiff and Class members are incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

69. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to millions of individuals' detailed PII and, thus, the significant number of individuals who would be harmed by the exposure of the

---

[25] *See* Caesars's Online Notice, *supra* n. 2.

[26] *See Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO-07-737, *supra* n. 20.

[27] *See Identity Theft.gov*, FTC, https://www.identitytheft.gov/Steps (last visited Aug. 15, 2023).

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

unencrypted data.

70. The injuries to Plaintiff and Class members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class members.

Impact of Identity Theft Can Have Ripple Effects

71. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, in addition to the irreparable damage that may result from the theft of a Social Security number, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. The Department of Justice's Bureau of Justice Statistics found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.

72. And, the impact of identity theft can have ripple effects, which can adversely affect the future financial trajectories of victims' lives. For example, the Identity Theft Resource Center reports that respondents to their surveys in 2013-2016 described that the identity theft they experienced affected their ability to get credit cards and obtain loans such as student loans or mortgages.[28] For some victims, this could mean the difference between going to college or not, becoming a homeowner or not, or having to take out a high interest payday loan versus a lower-interest loan.

73. It is no wonder then that identity theft exacts a severe emotional toll on its victims.

74. The 2017 Identity Theft Resource Center survey [29] evidences the emotional suffering experienced by victims of identity theft:

---

[28] *Identity Theft: The Aftermath 2017*, IDENTITY THEFT RES. CTR., https://www.idtheftcenter.org/wp-content/uploads/images/page-docs/Aftermath_2017.pdf (last visited Aug. 15, 2023).

[29] *Id.*

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

- 75% of respondents reported feeling severely distressed;
- 67% reported anxiety;
- 66% reported feelings of fear for the financial safety of family members;
- 24% reported fear for their physical safety;
- 15.2% reported that a relationship ended or was severely and negatively impacted by the identity theft; and
- 7% reported feeling suicidal.

75. Identity theft can also exact a physical toll on its victims. The same survey reported that respondents experienced physical symptoms stemming from their experience with identity theft:

- 48.3% of respondents reported sleep disturbances;
- 37.1% reported an inability to concentrate and/or lack of focus;
- 28.7% reported that they were unable to go to work because of physical symptoms;
- 23.1% reported new physical illnesses, including aches and pains, heart palpitations, sweating, and/or stomach issues;
- 12.6% reported a start or relapse into unhealthy or addictive behaviors.[30]

76. There may also be a significant time lag between when PII is stolen and when it is actually misused. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt

[30] *Id.*

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[31]

77. As the result of the Data Breach, Plaintiff and class members have suffered and/or will suffer or continue to suffer economic loss, a substantial risk of future identity theft, and other actual harm for which they are entitled to damages, including, but not limited to, the following:

- Losing the inherent value of their PII;
- Losing the value of Defendant's implicit promises of adequate data security;
- Identity theft and fraud resulting from the theft of their PII;
- Costs associated with the detection and prevention of identity theft and unauthorized use of their PII;
- Costs associated with purchasing credit monitoring and identity theft protection services;
- Unauthorized charges and loss of use of and access to their financial account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;
- Lowered credit scores resulting from credit inquiries following fraudulent activities;
- Costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including discovering fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposing withdrawal and purchase limits on compromised

[31] *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO-07-737, *supra* n. 20.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

accounts, and the stress, nuisance and annoyance of dealing with the repercussions of the Data Breach; and

- The continued imminent and certainly impending injury flowing from potential fraud and identify theft posed by their PII being in the possession of one or many unauthorized third parties.

78. Additionally, Plaintiff and Class members place significant value in data security.

79. Because of the value consumers place on data privacy and security, companies with robust data security practices can command higher prices than those who do not. Indeed, if consumers did not value their data security and privacy, companies like Defendant would have no reason to tout their data security efforts to their actual and potential customers.

80. Consequently, had consumers known the truth about Defendant's data security practices—that Defendants would not adequately protect and store their data—they would not have entrusted their PII to Defendant, purchased insurance that included Defendant's services, or paid as much for such services or benefits.

81. As such, Plaintiff and Class members did not receive the benefit of their bargain with Defendant because they entrusted their PII and purchased accommodations, dining, gaming and other goods and services with the reasonable expectation that Defendant would adequately protect and store their data, which it did not.

CLASS ACTION ALLEGATIONS

82. Plaintiff repeats and realleges each and every fact, matter, and allegation set forth above and incorporates them at this point by reference as though set forth in full.

83. Plaintiff brings this action on behalf of herself and the members of the proposed Class, which consists of:

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

All individuals residing in the United States whose personal identifiable information was compromised as a result of the Data Breach.

84. Excluded from the Class are Defendant, any entity in which Defendant has a controlling interest, and Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and members of their immediate families and judicial staff.

85. Plaintiff reserves the right to amend the above definition or to propose subclasses before the Court determines whether certification is appropriate.

86. **Numerosity**: The proposed Class is so numerous that joinder of all members is impracticable. Defendant has reported that the total number of individuals affected in the Data Breach may be in the tens of millions.

87. **Typicality**: Plaintiff's claims are typical of the claims of the Class. Plaintiff and all members of the Class were injured through Defendant's uniform misconduct. The same event and conduct that gave rise to Plaintiff's claims are identical to those that give rise to the claims of every other Class member because Plaintiff and each member of the Class had their sensitive PII compromised in the same way by the same conduct of Defendant.

88. **Adequacy**: Plaintiff is an adequate representative of the Class because Plaintiff's interests do not conflict with the interests of the Class; Plaintiff has retained competent counsel who are experienced in prosecuting complex class action and data breach class action litigation; and Plaintiff and Plaintiff's counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and his counsel.

89. **Superiority**: A class action is superior to all other available methods for the fair and efficient adjudication of this lawsuit because individual litigation of the claims of all members of

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

the Class is economically unfeasible and procedurally impracticable. The injury suffered by each individual member of the Class is relatively small in comparison to the burden and expense of individual prosecution of litigation. It would be very difficult for members of the Class to effectively redress Defendant's wrongdoing. Further, individualized litigation presents a potential for inconsistent or contradictory judgments.

90. **Commonality and Predominance**: There are numerous questions of law and fact common to the Class which predominate over any questions affecting only individual members of the Class.

91. Among the questions of law and fact common to the Class are:

a. Whether Defendant engaged in the wrongful conduct alleged herein;

b. Whether Defendant failed to adequately safeguard Plaintiff's and the Class's PII;

c. Whether Defendant failed to ensure the third-party vendor it hired had adequate data security, procedures, practices, and protocols;

d. Whether Defendant negligently hired and/or failed to supervise the third-party vendor it hired and gave access to Plaintiff's and the Class's PII;

e. Whether Defendant owed a duty to Plaintiff and the Class to adequately protect their PII, and whether it breached this duty;

f. Whether Defendant breached its duties to Plaintiff and the Class as a result of the Data Breach;

g. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach;

h. Whether Defendant was negligent in permitting the third-party access to Plaintiff's and the Class's PII;

i. Whether Defendant was negligent in failing to adhere to reasonable retention

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

policies, thereby greatly increasing the size of the Data Breach;

j. Whether Defendant failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiff and the Class;

k. Whether Defendant continues to breach duties to Plaintiff and the Class;

l. Whether Plaintiff and the Class suffered injury as a proximate result of Defendant's negligent actions or failures to act;

m. Whether Plaintiff and the Class are entitled to recover damages, equitable relief, and other relief; and

n. Whether Defendant's actions alleged herein constitute gross negligence, and whether Plaintiff and Class members are entitled to punitive damages.

CAUSES OF ACTION
FIRST CAUSE OF ACTION
NEGLIGENCE
(By Plaintiff and on Behalf of the Class)

92. Plaintiff repeats and realleges each and every fact, matter, and allegation set forth above and incorporates them at this point by reference as though set forth in full.

93. Defendant owed a duty of care to Plaintiff and Class members to use reasonable means to secure and safeguard the entrusted PII, to prevent its unauthorized access and disclosure, to guard it from theft, and to detect any attempted or actual breach of its systems, as alleged herein. These common law duties existed because Plaintiff and Class members were the foreseeable and probable victims of any inadequate security practices in Defendant's affirmative development and maintenance of its data security systems and its hiring of third-party providers entrusted with accessing, storing, safeguarding, handling, collecting, and/or protecting Plaintiff's and Class members' PII. In fact, not only was it foreseeable that Defendant and Class members would be

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

harmed by the failure to protect their PII because hackers routinely attempt to steal such information and use it for nefarious purposes, Defendant also knew that it was more likely than not that Plaintiff and other Class members would be harmed by such exposure and theft of their PII.

94. Defendant's duties to use reasonable security measures also arose as a result of a special relationship with Plaintiff and Class members as a result of being entrusted with their PII, which provided an independent duty of care. Plaintiff's and Class members' willingness to entrust Defendant with their PII was predicated on the understanding that Defendant would take adequate security precautions. Moreover, Defendant was capable of protecting its network and systems, and the PII it stored on them, from unauthorized access.

95. Defendant's duties to use reasonable data security measures also arose under Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect PII. Various FTC publications and data security breach orders further form the basis of Defendant's duties.

96. Defendant breached the aforementioned duties when it failed to use security practices that would protect the PII provided to it by Plaintiff and Class members, thus resulting in unauthorized exposure and access to Plaintiff's and Class members' PII.

97. Defendant further breached the aforementioned duties by failing to design, adopt, implement, control, manage, monitor, update, and audit its processes, controls, policies, procedures, and protocols to comply with the applicable laws and safeguard and protect Plaintiff's and Class members' PII within its possession, custody, and control.

98. As a direct and proximate cause of Defendant's failure to use appropriate security practices and failure to select a third-party provider with adequate data security measures, Mr. Plaintiff's and Class members' PII was exposed, disseminated, and made available to unauthorized

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

third parties.

99. Defendant admitted that Plaintiff's and Class members' PII was wrongfully disclosed as a result of the Data Breach.

100. The Data Breach caused direct and substantial damages to Plaintiff and Class members, as well as the likelihood of future and imminent harm through the dissemination of their PII and the greatly enhanced risk of credit fraud and identity theft.

101. By engaging in the foregoing acts and omissions, Defendant committed the common law tort of negligence. For all the reasons stated above, Defendant's conduct was negligent and departed from reasonable standards of care including by, but not limited to: failing to adequately limit access to and protect the PII; failing to conduct regular security audits; and failing to provide adequate and appropriate supervision of persons having access to Plaintiff's and Class members' PII.

102. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class members, their PII would not have been compromised.

103. Neither Plaintiff nor Class members contributed to the Data Breach or subsequent misuse of their PII as described in this Complaint.

104. As a direct and proximate result of Defendant's negligence, Plaintiff and Class members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach investigating

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

the nature of the Data Breach not fully disclosed by Defendant, reviewing bank statements, payment card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

SECOND CAUSE OF ACTION
NEGLIGENCE *PER SE*
(By Plaintiff and on Behalf of the Class)

105. Plaintiff repeats and realleges each and every fact, matter, and allegation set forth above and incorporates them at this point by reference as though set forth in full.

106. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by Defendant of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant's duty.

107. Defendant violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect PII and not complying with industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII obtained and stored and the foreseeable consequences of a data breach.

108. Defendant's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence *per se*.

109. Plaintiff and Class members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) were intended to protect.

110. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of Defendants' failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

Plaintiff and Class members.

111. As a direct and proximate result of Defendant's negligence, Plaintiff and Class members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach investigating the nature of the Data Breach not fully disclosed by Defendant, reviewing bank statements, payment card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

THIRD CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(By Plaintiff and on Behalf of the Class)

112. Plaintiff repeats and realleges each and every fact, matter, and allegation set forth above and incorporates them at this point by reference as though set forth in full.

113. Plaintiff and Class members entered into an implied contract with Caesars when they obtained products or services from Caesars, joined the loyalty program, or otherwise provided PII to Caesars.

114. As part of these transactions, Caesars agreed to safeguard and protect the PII of Plaintiff and Class members and to timely and accurately notify them if their PII was breached or compromised.

115. Plaintiff and Class members entered into the implied contracts with the reasonable expectation that Caesars's data security practices and policies were reasonable and consistent with

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

legal requirements and industry standards. Plaintiff and Class members believed that Caesars would use part of the monies paid to Caesars under the implied contracts or the monies obtained from the benefits derived from the PII they provided to fund proper and reasonable data security practices.

116. Plaintiff and Class members would not have provided and entrusted their PII to Caesars or would have paid less for Caesars products or services in the absence of the implied contract or implied terms between them and Caesars. The safeguarding of the PII of Plaintiff and Class members was critical to realize the intent of the parties.

117. Plaintiff and Class members fully performed their obligations under the implied contracts with Caesars.

118. Caesars breached its implied contracts with Plaintiff and Class members to protect their PII when it (1) failed to take reasonable steps to use safe and secure systems to protect that information; and (2) disclosed that information to unauthorized third parties.

119. As a direct and proximate result of Caesars's breach of implied contract, Plaintiff and Class members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of Caesars's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

FOURTH CAUSE OF ACTION
UNJUST ENRICHMENT

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

(In the alternative)
(By Plaintiff and on Behalf of the Class)

120. Plaintiff repeats and realleges each and every fact, matter, and allegation set forth above and incorporates them at this point by reference as though set forth in full.

121. This claim is pleaded in the alternative to the Breach of Implied contract claim set forth in the Third Cause of Action.

122. Plaintiff and Class members have an interest, both equitable and legal, in the PII about them that was conferred upon, collected by, and maintained by Defendant and that was ultimately stolen in the Data Breach.

123. Defendant benefitted from the conferral upon it of the PII pertaining to Plaintiff and Class members and by its ability to retain, use, sell, and profit from that information. Caesars understood that it was in fact so benefitted.

124. Caesars also understood and appreciated that the PII pertaining to Plaintiff and Class members was private and confidential and its value depended upon Caesars maintaining the privacy and confidentiality of that PII.

125. But for Caesars's willingness and commitment to maintain its privacy and confidentiality, Plaintiff and Class members would not have provided their PII to Caesars or would not have permitted Caesars to gather additional PII.

126. Plaintiff's and Class members' PII has an independent value to Caesars.

127. Caesars admits that it uses the PII it collects for, among other things, "administer[ing] and promot[ing] [its] business," "improv[ing] [its] products and services" and "product[ing] and defend[ing] [its] rights or property or enforce[ing] [its] agreement with [the member]," and that it uses its PII to "internal market research and analytics."[32]

128. Because of its use of Plaintiff's and Class members' PII, Caesars sold more services and products than it otherwise would have. Caesars was unjustly enriched by profiting from the

[32] https://www.caesars.com/corporate/privacy (last visited Oct. 10, 2023).

SJG STRANCH, JENNINGS & GARVEY PLLC
3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com

additional services and products it was able to market, sell, and create through the use of Plaintiff's and Class members' PII to the detriment of Plaintiff and Class members.

129. Caesars also benefitted through its unjust conduct by retaining money paid by Plaintiff and Class members that it should have used to provide proper data security to protect Plaintiff's and Class members' PII.

130. It is inequitable for Caesars to retain these benefits.

131. As a result of Caesars's wrongful conduct as alleged in this Complaint (including among other things its failure to employ proper data security measures, its continued maintenance and use of the PII belonging to Plaintiff and Class members without having proper data security measures, and its other conduct facilitating the theft of that PII), Caesars has been unjustly enriched at the expense of, and to the detriment of, Plaintiff and Class members.

132. Caesars's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiff's and Class members' sensitive PII, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identity thieves.

133. It is inequitable, unfair, and unjust for Caesars to retain these wrongfully obtained benefits. Caesars's retention of wrongfully obtained monies would violate fundamental principles of justice, equity, and good conscience.

134. The benefit conferred upon, received, and enjoyed by Caesars was not conferred officiously or gratuitously, and it would be inequitable, unfair, and unjust for Caesars to retain the benefit.

135. Caesars's defective security and its unfair and deceptive conduct have, among other things, caused Plaintiff and Class members to unfairly incur substantial time and/or costs to mitigate and monitor the use of their PII and has caused the Plaintiff and Class members other damages as described herein.

136. Plaintiff has no adequate remedy at law.

137. Caesars is therefore liable to Plaintiff and Class members for restitution or

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
SJG STRANCH, JENNINGS & GARVEY PLLC
725-235-9750
lasvegas@stranchlaw.com

disgorgement in the amount of the benefit conferred on Caesars as a result of its wrongful conduct, including specifically: the value to Caesars of the PII that was stolen in the Data Breach; the profits Caesars received and is receiving from the use of that information; the amounts that Caesars overcharged Plaintiff and Class members for use of Caesars's products and services; and the amounts that Caesars should have spent to provide proper data security to protect Plaintiff's and Class members' PII.

FIFTH CAUSE OF ACTION
BREACH OF CONFIDENCE
(By Plaintiff and on Behalf of the Class)

138. Plaintiff repeats and realleges each and every fact, matter, and allegation set forth above and incorporates them at this point by reference as though set forth in full.

139. Plaintiff and Class members maintained a confidential relationship with Caesars whereby Caesars undertook a duty not to disclose to unauthorized parties the PII that Plaintiff and Class members provide to Caesars. Such PII was confidential and novel, highly personal and sensitive, and not generally known.

140. Caesars knew Plaintiff's and Class members' PII was disclosed in confidence and understood the confidence was to be maintained, including by expressly and implicitly agreeing to protect the confidentiality and security of the PII it collected, stored, and maintained.

141. As a result of the Data Breach, there was an unauthorized disclosure of Plaintiff's and Class members' PII in violation of this understanding. The unauthorized disclosure occurred because Caesars failed to implement and maintain reasonable safeguards to protect the PII in its possession and failed to comply with industry-standard data security practices.

142. Plaintiff and Class members were harmed by way of an unconsented disclosure of their confidential information to an unauthorized third party.

143. But for Caesars's actions and inactions in violation of the parties' understanding of confidence, the PII of Plaintiff and Class members would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Caesars's actions and inaction were the direct and legal cause of the theft of Plaintiff's and Class members' PII, as well as the resulting

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

damages.

144. The injury and harm Plaintiff and Class members suffered was the reasonably foreseeable result of Caesars's unauthorized disclosure of Plaintiff's and Class members' PII. Caesars knew its computer systems and technologies for accepting, securing, and storing Plaintiff's and Class members' PII had serious security vulnerabilities because Caesars failed to observe even basic information security practices or correct known security vulnerabilities.

145. As a direct and proximate result of Caesars's breach of confidence, Plaintiff and Class members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of Caesars's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

146. By collecting and storing this PII and using it for commercial gain, Caesars has a duty of care to use reasonable means to secure and safeguard this PII to prevent disclosure and guard against theft of the PII.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Class pray for judgment against Defendant as follows:

a. An order certifying this action as a class action under Federal Rule of Civil Procedure 23, defining the Class as requested herein, appointing the undersigned as Class

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

Counsel, and finding that Plaintiff is a proper representative of the Class requested herein;

b. For injunctive and other equitable relief as necessary to protect the interests of Plaintiff and the Class as requested herein;

c. For an award of compensatory, consequential, and general damages, including nominal damages, as allowed by law in an amount to be determined;

d. For an award of restitution or disgorgement, in an amount to be determined;

e. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

f. For prejudgment interest on all amounts awarded; and

g. Such other and further relief as the Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all triable issues.

Dated: October 12, 2023

Respectfully submitted,

/s/ *Nathan Ring*
Nathan R. Ring,
Nevada State Bar No. 12078
STRANCH, JENNINGS & GARVEY, PLLC
3100 W. Charleston Boulevard, Suite 208
Las Vegas, NV 89102
Telephone: (725) 235-9750
nring@stranchlaw.com

Sabita J. Soneji (*pro hac vice forthcoming*)
TYCKO & ZAVAREEI LLP
1970 Broadway, Suite 1070
Oakland, CA 94612
Phone: (510) 254-6808
ssoneji@tzlegal.com

F. Peter Silva, II (*pro hac vice forthcoming*)
TYCKO & ZAVAREEI LLP
2000 Pennsylvania Avenue, NW, Suite 1010
Washington, D.C. 20006
Phone: (202) 973-0900

psilva@tzlegal.com

Counsel for Plaintiff and the Proposed Class
**Pro Hac Vice* application forthcoming

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC